

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЕРХНЕ-МОХОВИЧСКАЯ ОСНОВНАЯ ШКОЛА
ДЕМИДОВСКОГО РАЙОНА СМОЛЕНСКОЙ ОБЛАСТИ

ПРИКАЗ

от «11» апреля 2016 г.

№ 15 о/д

О регламенте работы в сети Интернет в МБОУ Верхне-Моховичской ОШ

В соответствии с Федеральным законом Российской Федерации от 29.12.2010 № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию», вступившем в силу с 01 сентября 2012 года, а так же в целях исключения доступа обучающихся к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами обучения и воспитания обучающихся, в соответствии с правилами подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, утвержденной Министерством образования и науки РФ от 11 мая 2011 года

ПРИКАЗЫВАЮ:

1. Назначить:

1.1. ответственным за доступ к сети Интернет и внедрение системы

контентной фильтрации в МБОУ Верхне-Моховичской ОШ учителя информатики Карпенкова В.С.

1.2. ответственным за организацию антивирусной защиты в школе учителя информатики Карпенкова В.С.;

1.3. ответственным оператором электронной почты школы заместителя директора по УВР Лосич Е.В..

2. Утвердить:

2.1. Правила организации доступа МБОУ Верхне-Моховичской ОШ к информационным ресурсам посредством сети Интернет (приложение 1);

2.2. Инструкцию для сотрудников школы о порядке действий при осуществлении контроля над использованием обучающимися сети Интернет (приложение 2);

2.3. Должностную инструкцию лица, ответственного за доступ к школьной сети Интернет и внедрение системы контентной фильтрации (приложение 3);

2.4. Должностную инструкцию учителя при работе обучающихся в сети Интернет (приложение 4);

2.5. Классификатор информации, несовместимой с задачами обучения и воспитания (приложение 5);

2.6. Регламент работы с электронной почтой в МБОУ Верхне-Моховичской ОШ (приложение 6);

2.7. Инструкцию по организации антивирусной защиты (приложение 7).

2.8. Положение о школьной локальной сети (приложение 8).

2.9. Правила пользования локальной сетью и сетью Интернет (приложение 9)

3. Учителю информатики Карпенкову В.С.:

3.1. осуществлять систематическую поддержку программы фильтрации доступа в Интернет (СКФ) с целью ограничения доступа к Интернет-ресурсам, содержание которых несовместимо с задачами воспитания и образования, ограничения нецелевого использования Интернет и сбора статистических сведений об использовании ресурсов Интернет обучающимися или иными пользователями;

3.2. при работе с сетью Интернет руководствоваться локальными актами МБОУ Верхне-Моховичской ОШ, перечисленными в п. 2 данного приказа.

4. Заместителю директора по УВР Лосич Е.В.:

4.1. ознакомить педагогов школы с локальными актами, отражёнными в п.п. 2.1, 2.2, 2.4 настоящего приказа;

4.2. проводить разъяснительную работу с педагогическим коллективом школы по вопросам классификации информации, распространение которой запрещено в соответствии с законодательством Российской Федерации и информации, несовместимой с задачами образования и воспитания(постоянно);

4.3. осуществлять контроль за внедрением в школе организационных механизмов исключения доступа обучающихся к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания обучающихся.

5. В соответствии с положением о регламенте работы в школьной сети Интернет провести инструктаж с обучающимися: учителю информатики – на уроках информатики, классным руководителям – на классных часах.

6. Возложить ответственность за пользование учащимися ресурсами сети Интернет: в кабинете информатики - на преподавателя информатики Карпенкова В.С.

7. Контроль исполнения настоящего приказа оставляю за собой.

Директор школы:

Н.А. Шамкова

**Правила
организации доступа МБОУ Верхне-Моховичской ОШ Демидовского
района Смоленской области к информационным ресурсам
посредством сети Интернет**

1. Общие положения

1.1. Настоящие Правила регулируют условия и порядок использования сети Интернет обучающимися, преподавателями и сотрудниками муниципального бюджетного общеобразовательного учреждения Верхне-Моховичская ОШ и утверждается приказом директора.

1.2. Доступ к сети Интернет должен осуществляться только с использованием лицензионного программного обеспечения или программного обеспечения, разрешенного для свободного использования.

1.3. Использование школьной сети Интернет направлено на решение задач образовательного процесса и подчинено следующим принципам:

- соответствия образовательным целям;
- содействия гармоничному формированию и развитию личности;
- уважения закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернета;
- приобретения новых навыков и знаний;
- расширения применяемого спектра учебных и наглядных пособий;
- социализации личности, введения в информационное общество.

1.4. Использование сети Интернет в образовательном учреждении должно осуществляться в соответствии с:

- законодательством Российской Федерации;
- опытом целесообразной и эффективной организации учебного процесса с использованием информационных технологий и возможностей Интернета;
- интересами обучающихся;
- целями образовательного процесса;
- рекомендациями профильных органов и организаций в сфере классификации ресурсов Сети.

1.5. При организации доступа к информационным ресурсам сети Интернет

ответственные лица школы должны руководствоваться:

- Конституцией Российской Федерации (Собрание законодательства Российской Федерации, 2009, № 4 ст. 445);
- Законом Российской Федерации от 29.12.2012г № 273-ФЗ «Об образовании»

- Постановлением Правительства Российской Федерации от 7 февраля 2011 года № 61 «О федеральной целевой программе развития образования на 2011-2015 годы»;
- Федеральным законом Российской Федерации от 25 июля 2002г. №11-ФЗ «О противодействии экстремистской деятельности»;
- Федеральным законом от 7 июля 2003 года № 126-ФЗ «О связи»;
- Федеральным законом от 7 февраля 1992 года № 2300-1 «О защите прав потребителей»;
- Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом Российской Федерации от 29 декабря 2010 г. №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральным законом Российской Федерации от 21 июля 2011 г. №252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию"»;
- Федеральным законом Российской Федерации от 28 июля 2012 г. N 139-ФЗ «О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации»;
- Постановлением Правительства РФ от 23 января 2006 года №32 «Об утверждении правил оказания услуг связи по передаче данных»;
- Постановлением Правительства РФ от 10 сентября 2007 года №575 «Об утверждении правил оказания телематических услуг связи»;

2. Организация использования сети Интернет в МОУ школе.

2.1. Директор МБОУ Дубровская СШ отвечает за обеспечение участникам образовательного процесса эффективного и безопасного доступа к сети Интернет в школе, а также за внедрение соответствующих технических, правовых и иных механизмов.

2.2. Непосредственное определение политики доступа в Интернет осуществляет заместитель директора по УВР.

2.3. Для обеспечения доступа участников образовательного процесса к сети Интернет в соответствии с данными Правилами директор школы назначает своим приказом ответственного за доступ к сети Интернет и внедрение системы контентной фильтрации.

2.4. Использование сети Интернет сотрудниками школы возможно исключительно при условии ознакомления с настоящими Правилами.

2.5. Вопросы использования возможностей сети Интернет в образовательном процессе и доступа к ресурсам Интернет обучающихся рассматриваются на педагогическом Совете по вопросам регламентации доступа к информации в сети Интернет.

2.6. Принятие решений о разрешении/блокировании доступа к ресурсам/группам ресурсов сети Интернет осуществляется заместителем директора по УВР, курирующим вопросы информатизации совместно с ответственным за доступ к сети Интернет и внедрение системы контентной фильтрации в школе.

2.7. Во время уроков и других занятий контроль над использованием обучающимися ресурсов сети Интернет в соответствии с настоящими Правилами осуществляет учитель, ведущий занятие.

При этом учитель:

- наблюдает за использованием компьютера и сети Интернет обучающимися;
- запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения им настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в образовательном учреждении;
- принимает предусмотренные настоящими Правилами и иными нормативными документами меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

2.8. Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль над использованием ресурсов Интернета осуществляют работники школы (заместитель директора по УВР, учителя-предметники), определенные приказом директора, которые:

- определяют время и место для свободной работы в сети Интернет обучающихся, преподавателей и сотрудников школы с учетом использования соответствующих технических мощностей школы в образовательном процессе, а также длительность сеанса работы одного человека;
- контролируют объем трафика в сети Интернет;
- наблюдают за использованием компьютера и сети Интернет обучающимися;
- принимают предусмотренные настоящими Правилами, Инструкцией о порядке

действий при осуществлении контроля за использованием обучающимися сети Интернет и иными нормативными документами меры по пресечению

обращений к ресурсам, не имеющим отношения к образовательному процессу;

- запрещают дальнейшую работу пользователя в сети Интернет в случае нарушения пользователем настоящих Правил;
- сообщают заместителю директора по УВР о преднамеренных попытках обучающегося осуществить обращение к ресурсам, не имеющим отношения к образовательному процессу, о случаях нарушения обучающимися установленных Правил пользования Интернетом.

2.9. При использовании школьной сети Интернет обучающимся предоставляется доступ только к тем ресурсам, содержание которых не

противоречит законодательству Российской Федерации и не является несовместимым с целями и задачами образования и обучения.

Проверка выполнения такого требования осуществляется с помощью специальных

технических средств и программного обеспечения контентной фильтрации,

установленного в школьных компьютерах.

2.10. Использование школьной сети Интернет без применения данных технических средств и программного обеспечения (например, в случае технического отказа) допускается только для лиц, достигших 18 лет, с индивидуального разрешения директора школы.

2.11. Пользователи сети Интернет должны учитывать, что технические средства и программное обеспечение не могут обеспечить полную фильтрацию ресурсов сети Интернет вследствие частого обновления ресурсов. В связи с этим существует вероятность обнаружения обучающимися ресурсов, не имеющих отношения к образовательному процессу и содержание которых противоречит законодательству Российской Федерации. Участникам использования сети Интернет следует осознавать, что школа не несет ответственности за случайный доступ к подобной информации, размещенной не на школьных Интернет-ресурсах. При обнаружении указанной информации пользователю необходимо сообщить

об этом ответственному за доступ к сети Интернет и внедрение системы

контентной фильтрации в школе, или непосредственно заместителю директора по УВР, указав при этом адрес ресурса.

2.12. Принципы размещения информации на Интернет-ресурсах школы призваны обеспечивать:

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защиту персональных данных обучающихся, преподавателей и сотрудников;
- достоверность и корректность информации.

2.13. Персональные данные обучающихся (включая фамилию и имя, класс/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные сведения личного характера) могут размещаться на интернет-ресурсах, создаваемых школой, только с письменного согласия родителей или иных законных представителей обучающихся. Персональные данные преподавателей и сотрудников школы размещаются на Интернет-ресурсах школы только с письменного согласия лица, чьи персональные данные размещаются.

2.14. В информационных сообщениях о мероприятиях, размещенных на школьном сайте без уведомления и получения согласия упомянутых лиц или их законных представителей, могут быть указаны лишь фамилия и имя

обучающегося либо фамилия, имя и отчество преподавателя, сотрудника или родителя.

2.15. При получении согласия на размещение персональных данных представитель школы обязан разъяснить возможные риски и последствия их опубликования. Школа не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

3. Использование сети Интернет в школе.

3.1. Использование сети Интернет осуществляется, как правило, в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области сети Интернет и компьютерной грамотности лицо может осуществлять доступ к ресурсам необразовательной направленности.

3.2. По разрешению заместителя директора по УВР преподаватели, сотрудники и обучающиеся (с согласия родителей законных представителей) вправе:

- размещать собственную информацию в сети Интернет на Интернет-ресурсах школы;
- иметь учетную запись электронной почты на школьных интернет-ресурсах или на общедоступных серверах электронной почты, если они не включены в перечень Интернет-ресурсов, доступ к которым ограничен.

3.3. При работе с ресурсами сети Интернет недопустимо:

- распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;
- публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого

компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

3.4. Обучающимся, преподавателям и сотрудникам запрещается:

- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
- использовать программные и аппаратные средства, позволяющие получить доступ к ресурсам сети Интернет, содержание которых не имеет отношения к образовательному процессу, а так же к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством включая материалы, носящие вредоносную,

угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

- обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
- осуществлять любые сделки через Интернет;
- осуществлять загрузки файлов на компьютер школы без специального разрешения;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.5. При случайном обнаружении пользователем, работающим в сети Интернет, ресурса, содержимое которого несовместимо с целями образовательного процесса, он обязан незамедлительно сообщить о таком ресурсе заместителю директора по УВР либо лицу, ответственному за доступ к сети Интернет и внедрение системы контентной фильтрации в школе с указанием его доменного адреса и покинуть данный ресурс.

3.6. Заместитель директора по УВР либо ответственный за доступ к сети Интернет и внедрение системы контентной фильтрации обязаны:

- принять информацию от пользователя;
- предпринять соответствующие меры по блокированию запрещённого контента;
- довести информацию до сведения директора школы.

к приказу по Верхне-Моховичской ОШ
от 11.04.2016 № 15о/д

**Инструкция для сотрудников МБОУ Верхне-Моховичской ОШ
Демидовского района Смоленской области о порядке действий при
осуществлении контроля над использованием
обучающимися сети Интернет**

1. Настоящая инструкция устанавливает порядок действий сотрудников школы по вопросам регламентации доступа к информации в Интернете при обнаружении:

- обращения обучающихся к контенту, не имеющему отношения к образовательному процессу;
- отказа при обращении к контенту, имеющему отношение к образовательному процессу, вызванного техническими причинами.

2. Контроль за использованием обучающимися сети Интернет осуществляют:

- во время занятия — проводящий его учитель;
- во время использования сети Интернет для свободной работы обучающихся — сотрудники, назначенные директором школы.

3. Учитель, а также лицо, осуществляющее контроль за использованием обучающимися сети Интернет:

- определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательном процессе соответствующих технических возможностей, а также длительность сеанса работы одного обучающегося;
- наблюдает за использованием обучающимися компьютеров и сети Интернет;
- способствует осуществлению контроля объемов трафика школы в сети Интернет;
- запрещает дальнейшую работу обучающегося в сети Интернет на уроке (занятии) в случае нарушения им порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;
- не допускает обучающегося к работе в Интернете в случаях, предусмотренных

Регламентом организации доступа к информационным ресурсам посредством сети Интернет;

- доводит до классного руководителя информацию о нарушении обучающимся правил работы в сети Интернет;
- принимает необходимые меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

4. При обнаружении ресурса, который, по мнению учителя содержит информацию, запрещенную для распространения в соответствии с законодательством Российской Федерации, или иного потенциально опасного для обучающихся контента, а также при обнаружении того, что доступ к необходимому для организации образовательного процесса Интернет-ресурсу запрещен, сотрудник школы сообщает об этом лицу, ответственному за доступ к сети Интернет и внедрение системы контентной фильтрации или непосредственно заместителю директора по УВР.

5. Заместитель директора по УВР совместно с ответственным лицом за доступ к сети Интернет и внедрение системы контентной фильтрации проверяют ресурс, принимают необходимые решения по изменению прав доступа к соответствующим Интернет-ресурсам и сообщают о данном факте директору школы.

7. При обнаружении вызванного техническими причинами отказа доступа к контенту, не представляющему опасности для обучающихся, доступ к которому не противоречит принятым нормативным актам на федеральном уровне, ответственное лицо принимает соответствующие меры по восстановлению доступа к разрешенному контенту или по блокированию запрещённого контента и сообщает о неверной категоризации ресурса в службу технической поддержки СКФ по специальной «горячей линии» на сайте Экспертного педагогического сообщества <http://skf.edu.ru>.

к приказу по МБОУ Верхне-Моховичской ОШ

от 11.04. 2016 г. № 15 о/д

**Должностная инструкция лица, ответственного за доступ к сети
Интернет и внедрение системы контентной фильтрации
в МБОУ Верхне-Моховичской ОШ Демидовского района
Смоленской области**

Ответственный за доступ к сети Интернет и внедрение системы контентной фильтрации назначается приказом директора школы.

1. Общие положения

Должен знать:

- дидактические возможности использования ресурсов сети Интернет;

- правила безопасного использования сети Интернет.

2. Должностные обязанности:

- планирует использование ресурсов в школьной сети Интернет на основании заявок учителей;

- организует получение сотрудниками школы электронных адресов и паролей для работы в сети Интернет и информационной среде школы;

- организует контроль использования сети Интернет;

- принимает меры по восстановлению доступа к разрешенному контенту или по блокированию запрещённого контента в сети Интернет;

- организует контроль работы оборудования и программных средств, обеспечивающих использование сети Интернет и ограничение доступа;

- систематически повышает свою профессиональную квалификацию, общепедагогическую и предметную компетентность, включая ИКТ-компетентность, компетентность в использовании возможностей Интернета в образовательном процессе;

- обеспечивает информирование организаций, отвечающих за работу технических и программных средств, об ошибках в работе оборудования и программного обеспечения;

- соблюдает правила и нормы охраны труда, техники безопасности и противопожарной защиты, правила использования сети Интернет.

3. Ответственность

Несет ответственность за выполнение регламента организации доступа к ресурсам сети Интернет и ограничения доступа, установленного в школе.

**Должностная инструкция учителя
при работе обучающихся МБОУ Верхне-Моховичской ОШ
Демидовского района Смоленской области
в сети Интернет
(внесения изменений в должностные инструкции)**

1. Общие положения

Должен знать:

- дидактические возможности использования ресурсов сети Интернет;
- правила безопасного использования сети Интернет.

2. Должностные обязанности:

- планирует использование ресурсов сети Интернет в учебном процессе

с учетом специфики преподаваемого предмета;

- разрабатывает, согласует с методическим объединением, представляет на педагогическом совете школы и размещает в информационном пространстве школы календарно-тематическое планирование;

- получает и использует в своей деятельности электронный адрес и пароли

для работы в сети Интернет ;

- использует разнообразные приемы, методы и средства обучения, в том числе возможности сети Интернет;

- во время ведения уроков и других занятий осуществляет контроль над использованием обучающимися ресурсов сети Интернет;

- систематически повышает свою профессиональную квалификацию, общепедагогическую и предметную компетентность, включая ИКТ-компетентность, компетентность в использовании возможностей Интернета в учебном процессе;

- соблюдает правила и нормы охраны труда, техники безопасности и противопожарной защиты, регламент организации доступа к информационным ресурсам посредством сети Интернет.

3. Права

Вправе определять ресурсы сети Интернет, используемые обучающимися в учебном процессе.

4. Ответственность

Несет ответственность за выполнение обучающимися правил доступа к ресурсам сети Интернет в ходе учебного процесса.

Приложение 5
к приказу по
Верхне-Моховичской ОШ
от 11.04.2016 № 15 о/д

Классификатор информации, не имеющей отношения к образовательному процессу

1. Классификацию информации, запрещенной законодательством Российской Федерации к распространению и не имеющей отношения к образовательному процессу, осуществляют специальные экспертно-консультативные органы (советы) при органах управления образованием.
2. Классификатор информации, запрещенной законодательством Российской Федерации к распространению, применяется в единообразном виде на всей территории Российской Федерации.
3. Классификатор информации, не имеющей отношения к образовательному процессу, может содержать как части (разделы), рекомендуемые к применению в единообразном виде на всей территории Российской Федерации, так и части (разделы), рекомендуемые к использованию экспертно-консультативными органами (советами) регионального и (или) муниципального уровня.
4. В соответствии с законодательством Российской Федерации образовательное учреждение свободно в выборе и применении классификаторов информации, не имеющей отношения к образовательному процессу, а также несет ответственность за невыполнение функций, отнесенных к его компетенции.
5. Рекомендации по формированию Классификатора информации, распространение которой запрещено в соответствии с законодательством Российской Федерации, разработаны в соответствии с проведенным анализом законодательства Российской Федерации и международных договоров Российской Федерации.

№ п/п	Тематическая категория	Содержание
1	Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения	- Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; - информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию токсикоманию, антиобщественное поведение
2	Злоупотребление свободой СМИ — экстремизм	Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы
3	Злоупотребление свободой СМИ — наркотические средства	Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров
4	Злоупотребление свободой СМИ — информация с ограниченным доступом	Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций
5	Злоупотребление свободой СМИ — скрытое воздействие	Информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающая вредное влияние на их здоровье
6	Экстремистские материалы или экстремистская	А) Экстремистские материалы, то есть предназначенные для обнародования документы или информация, призывающие к

	деятельность (экстремизм)	осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии; публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы; Б) экстремистская деятельность (экстремизм) включает деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков: - насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации; - подрыв безопасности Российской Федерации, захват или присвоение властных полномочий, создание незаконных вооруженных формирований; - осуществление террористической деятельности либо публичное оправдание терроризма; - возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию; - унижение национального достоинства; - осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы; - пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к
--	--------------------------------------	---

7	Вредоносные программы	религии, социальной, расовой, национальной, религиозной или языковой принадлежности; - воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, сопровождаемое насилием или угрозой его применения; - публичная клевета в отношении лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, сопровождаемая обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке; - применение насилия в отношении представителя государственной власти либо угроза применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей; - посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность; - нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением Программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети - Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его
---	-----------------------	--

8	Преступления	репутацию); - оскорбление (унижение чести и достоинства другого лица, выраженное в неприличной форме); - публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма; - склонение к потреблению наркотических средств и психотропных веществ; - незаконное распространение или рекламирование порнографических материалов; - публичные призывы к осуществлению экстремистской деятельности; - информация, направленная на пропаганду национальной, классовой, социальной нетерпимости, а также социального, расового, национального и религиозного неравенства; - публичные призывы к развязыванию агрессивной Войны. Информация, содержащая рекламу алкогольной продукции и табачных изделий Информация, составляющая государственную, коммерческую, служебную или иную охраняемую законом тайну
9	Ненадлежащая реклама	
10	Информация с ограниченным доступом	

6. Приводимый далее перечень категорий Классификатора информации, не имеющей отношения к образовательному процессу, носит рекомендательный характер и может быть дополнен, расширен или иным образом изменен в установленном порядке, в том числе с учетом

специфики образовательного учреждения, социокультурных особенностей автономного округа и иных обстоятельств.

<i>№ п/п</i>	<i>Тематическая категория</i>	<i>Содержание</i>
1	Алкоголь	Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию
2	Баннеры и рекламные программы	Баннерные сети, всплывающая реклама, рекламные программы
3	Вождение и автомобили (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям
4	Досуг и развлечения (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация: - фотоальбомы и фотоконкурсы; - рейтинги открыток, гороскопов, сонников; - гадания, магия и астрология; - ТВ-программы; - прогнозы погоды; - тесты, конкурсы онлайн; - туризм, путешествия; - тосты, поздравления; - кроссворды, сканворды, ответы к ним; - фантастика; - кулинария, рецепты, диеты; - мода, одежда, обувь, модные аксессуары, показы мод; - тексты песен, кино, киноактеры, расписания концертов, спектаклей, кинофильмов, заказ билетов в театры, кино и т.п.; - о дачах, участках, огородах, садах, цветоводстве, животных, питомцах, уходе за ними; - о рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах, увлечениях, хобби, коллекционировании; - о службах знакомств, размещении

		объявлений онлайн; - анекдоты, «приколы», слухи; - о сайтах и журналах для женщин и для мужчин; - желтая пресса, онлайн-ТВ, онлайн-радио; - о знаменитостях; - о косметике, парфюмерии, прическах, ювелирных украшениях.
5	Здоровье и медицина(ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иные материалы на тему «Здоровье и медицина», которые, являясь академическими, по сути, могут быть также отнесены к другим категориям (порнография, трупы и т.п.)
6	Компьютерные игры (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющие отношения к образовательному процессу компьютерные онлайн-овые и оффлайн-овые игры, советы для игроков и ключи для прохождения игр, игровые форумы и чаты
7	Корпоративные сайты, интернет-представительства негосударственных учреждений(ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, сайты коммерческих фирм, компаний, предприятий, организаций
8	Личная и немодерируемая информация	Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги
9	Отправка SMS с использованием интернет-ресурсов	Сайты, предлагающие услуги по отправке SMS-сообщений

10	Модерируемые доски объявлений (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты
11	Нелегальная помощь школьникам и студентам	Банки готовых рефератов, эссе, дипломных работ и пр.
12	Неприличный и грубый юмор	Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека
13	Нижнее белье, купальники	Сайты, на которых рекламируется и изображается нижнее белье и купальники
14	Обеспечение анонимности пользователя, обход контентных фильтров	Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам; Peer-to-Peer программы, сервисы бесплатных прокси-серверов, сервисы, дающие пользователю анонимность
15	Онлайн-казино и тотализаторы	Электронные казино, тотализаторы, игры на деньги, конкурсы и пр.
16	Платные сайты	Сайты, на которых вывешено объявление о платности посещения веб-страниц
17	Поиск работы, резюме, вакансии (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-представительства кадровых агентств, банки вакансий и резюме
18	Поисковые системы (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-каталоги, системы поиска и навигации в Интернете

19	Религии и атеизм (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Сайты, содержащие, не имеющую отношения к образовательному процессу, информацию религиозной и антирелигиозной направленности.
20	Системы поиска Изображений	Системы для поиска изображений в Интернете по ключевому слову или словосочетанию
21	СМИ (ресурсы данной категории, не имеющие отношения к образовательному процессу)	СМИ, содержащие новостные ресурсы и сайты СМИ (радио, телевидения, печати), не имеющие отношения к образовательному процессу.
22	Табак, реклама табака, пропаганда потребления табака	Сайты, пропагандирующие потребление табака; реклама табака и изделий из него
23	Торговля и реклама (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие, не имеющие отношения к образовательному процессу, сайты следующих категорий: аукционы, распродажи онлайн, интернет-магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги, иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, недвижимость, аренда недвижимости, покупка недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в Интернете, е-бизнес
24	Убийства, насилие	Сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.
25	Чаты (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Сайты для анонимного общения в режиме онлайн

Приложение 6
к приказу по
Верхне-Моховичской ОШ
от 11.04.2016 № 15 о/д

Регламент работы с электронной почтой в МБОУ Верхне-Моховичской ОШ

Общие положения

1.1. Муниципальное бюджетное общеобразовательное учреждение Верхне-Моховичская основная школа Демидовского района Смоленской области (далее МБОУ Верхне-Моховичская ОШ) имеет свой адрес электронной почты: sk_mohovichichi@rambler.ru

1.2. Электронная почта в школе может использоваться только в административных и образовательных целях.

1.3. Пользователи и владельцы электронных почтовых ящиков должны соблюдать правила и инструкции по работе с электронной почтой, этические нормы общения.

1.4. Перед отправлением сообщения или отчета необходимо проверить правописание и грамматику текста.

1.5. Пользователям данного сервиса запрещено:

- участвовать в рассылке посланий, не связанных с образовательной или административной деятельностью школы;
- пересылать по произвольным адресам не затребованную потребителями информацию (спам);
- отправлять сообщения противозаконного или неэтического содержания;
- использовать массовую рассылку электронной почты, за исключением необходимых случаев;
- электронное послание не должно использоваться для пересылки секретной и конфиденциальной информации, регламент обмена которыми утверждается иными нормативно-правовыми актами.

2. Порядок обработки, передачи и приёма документов по электронной почте

2.1. По электронной почте производится получение и отправка информации законодательного, нормативно-правового, учебного, учебно-методического характера, а также любой другой информации, совместимой с процессом образования

2.2. Для обработки, передачи и приема информации по электронной почте в школе приказом директора назначается ответственное лицо – оператор электронной почты.

2.3. При создании электронного почтового ящика (ЭПЯ), школьного сайта ответственное лицо направляет в муниципальный орган управления образованием

свои электронные реквизиты для формирования базы данных образовательных учреждений муниципалитета.

2.4. Администрация школы должна обеспечить бесперебойное функционирование сервиса электронной почты и регулярное получение и отpravку информации в течение всего рабочего дня.

2.5. Ответственность за ненадлежащую подготовку информации к передаче по электронной почте несет автор информации, предполагаемой к отправке.

2.6. Ответственность за отправку адресату и получение электронной почты – несет оператор электронной почты.

2.7. Передаваемые с помощью электронной почты официальные документы должны иметь исходящий регистрационный номер.

2.8. Размер вложения почтового сообщения не должен превышать 6 Мбайт.

2.9. Все передаваемые учебно-методические и справочно-информационные материалы должны передаваться с сопроводительным письмом. Для отправки электронного сообщения пользователь оформляет документ в соответствии с требованиями по делопроизводству, утвержденными в школе.

2.10. При получении электронного сообщения оператор:

- передает документ на рассмотрение администрации или в случае именного сообщения - непосредственно адресату;
- в случае невозможности прочтения электронного сообщения уведомляет об этом отправителя.

2.11. Отправка и получение электронных документов осуществляется с использованием программных продуктов, предназначенных для работы с электронной почтой в МБОУ Верхне-Моховичская ОШ

2.12. Учет электронных документов осуществляется путем регистрации в журнале регистрации входящих / исходящих документов.

2.13. Электронные документы дублируются в виде копий на бумажных носителях с присвоением номера входящего или исходящего документа. Сроки их хранения регламентируются иными нормативными актами.

3. Ответственность

3.1. Изменение наименования официального ЭПЯ школы согласовывает со специалистами муниципального органа управления образованием,

ведущими электронный документооборот и отвечающими за информатизацию системы муниципального образования.

3.2. По факту изменения официального ЭПЯ школа обязана уведомить информационным письмом орган управления образованием за 3 рабочих дня до смены ЭПЯ с указанием даты, с которой изменения вступают в силу.

3.3. Ответственность за функционирование электронного документооборота в МБОУ Верхне-Моховичской ОШ учреждении несет директор школы.

Приложение 7
к приказу по
Верхне-Моховичской ОШ
от 11.04.2016 № 15 о/д

Инструкция по организации антивирусной защиты в МБОУ Верхне-Моховичской ОШ

Общие положения

1.1. Настоящая инструкция предназначена для организации порядка проведения антивирусного контроля в муниципальном общеобразовательном учреждении «Дубровская средняя школа» и предотвращения возникновения фактов заражения программного обеспечения компьютерными вирусами, а также фильтрации доступа пользователей к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

1.2. Директором школы назначается лицо, ответственное за организацию антивирусной защиты компьютерной сети.

1.3. В школе может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

1.4. Установка, настройка и регулярное обновление антивирусных средств осуществляется только ответственным за организацию антивирусной защиты.

1.5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (магнитных дисках, лентах, CD-ROM, DVD, flash-накопителях и т.п.).

1.6. Контроль информации на съёмных носителях производится непосредственно перед её использованием.

1.7. Файлы, помещаемые в электронный архив или на сервер, должны в обязательном порядке проходить антивирусный контроль.

1.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

1.9. Факт выполнения антивирусной проверки должен регистрироваться в специальном журнале за подписью лица, ответственного за организацию антивирусной защиты.

2. Мероприятия, направленные на решение задач по антивирусной защите

2.1. Установка только лицензированного программного обеспечения либо бесплатного антивирусного программного обеспечения.

2.2. Регулярное обновление и профилактические проверки (обновление ежедневное; профилактические проверки: 1 раз в неделю во вторник с 12.00).

2.3. Непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах информационно-коммуникационной системы (далее ИКС) школы.

2.4. Проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.

2.5. Внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования.

2.6. Необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.

2.7. Обеспечение бесперебойной работы для случаев вирусного заражения, в том числе резервного копирования всех необходимых данных и программ и их восстановления.

3. Требования к проведению мероприятий по антивирусной защите

3.1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС – при перезагрузке) в автоматическом режиме должно выполняться

обновление антивирусных баз и серверов и проводится антивирусный контроль всех дисков и файлов персонального компьютера и съёмных носителей.

3.2. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

3.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

3.3.1. непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети) должна быть выполнена

антивирусная проверка на серверах и персональных компьютерах школы при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.);

3.3.2. при отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

4. Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

4.1.1. приостановить работу;

4.1.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты в школе совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

4.1.3. провести лечение или уничтожение зараженных файлов.

4.2. При возникновении подозрения на наличие компьютерного вируса ответственный за организацию антивирусной защиты должен провести внеочередной антивирусный контроль.

5. Ответственность

5.1. Ответственность за организацию антивирусной защиты и выполнение положений данной инструкции возлагается на лицо, назначенное директором школы.

5.2. Ответственность за проведение мероприятий антивирусного контроля в школе возлагается на ответственного за организацию антивирусной защиты.

5.3. Ответственность за соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

5.4. Периодический контроль за состоянием антивирусной защиты осуществляется директором школы и фиксируется Актом проверки (не реже 1 раз в квартал).

Положение о школьной локальной сети

Локальная сеть - компьютерная сеть, объединяющая некоторое количество компьютеров, позволяющих работать с сетевыми приложениями и осуществлять выход в Интернет через один IP адрес. Компьютерная сеть - часть единого информационного пространства школы, целостная структура, функционирование которой требует реализации организационно-технических мероприятий, жесткой дисциплины пользователей.

1. Назначение

Локальная сеть школы является неотъемлемой частью образовательной системы и предназначена для решения задач управления образовательным процессом на базе современных информационных технологий, обеспечивающих принятие решений на основе:

- оперативного обмена данными между участниками учебно-образовательного процесса;
- использования общих информационных ресурсов сети;
- доступа через единую компьютерную сеть к данным других Интрасетей и Интерсетей;
- использования электронной почты;
- организации централизованного хранилища данных с различным уровнем доступа к информации;

2. Состав

Локальную сеть образуют базовые компоненты оборудования, программного обеспечения и параметров сетевого и межсетевого взаимодействия:

2.1.Серверы:

- файловые; - баз данных; - приложений; - архивные;
- удаленного доступа; - почтовые; - прокси-серверы.

2.2.Телекоммуникационная инфраструктура:

- кабели; - соединительные устройства;
- устройства расширения (и ограничения) доступа; - межсетевые экраны;

2.3.Компьютеры с необходимыми сетевыми адаптерами.

2.4.Системы дублирования и хранения информации.

2.5.Системы бесперебойного питания серверов.

2.6.Информационная инфраструктура:

- операционные системы;
- протоколы сетевого и межсетевого взаимодействия;
- прикладное программное обеспечение коллективного доступа;

- прикладное программное обеспечение компьютеров.

3. Принцип действия

3.1. Функционирование сети обеспечивается подключением компьютеров к серверам и объединением серверов посредством соединительной аппаратуры.

3.2. Расширение сети производится путем подключения дополнительных сегментов через маршрутизаторы и каналы связи различного типа.

3.3. Подключение к сети Интернет производится через специализированные устройства и специализированное программное обеспечение для защиты внутренней сети от несанкционированного доступа.

3.4. Защита информации по уровням доступа производится путем администрирования файл-серверов и серверов баз данных, разграничения доступа к ресурсам сети и проведением специализированных организационно-технических мероприятий.

4. Функционирование

4.1. Все вопросы, касающиеся функционирования и развития локальной сети, решаются директором школы и регламентируются настоящим положением.

5. Сопровождение

5.1. Серверы.

- Отключение серверов или компьютеров для технологических целей производится только системным администратором с обязательным предварительным уведомлением всех пользователей ресурсов данного сервера.

5.2. Телекоммуникации.

- Создание и сопровождение телекоммуникационных каналов сети является исключительной компетенцией школы.

- Подключение персональных компьютеров к сети производится системным администратором отдела по образованию.

- Решение о подключении или реорганизации сегмента принимается системным администратором на основании заявки в соответствии с имеющимися ресурсами и техническими возможностями.

- Изменение типологии сети самостоятельно пользователем, подключение и реконфигурация любого элемента сети запрещено.

- Подключение модемов и иных устройств на компьютерах для доступа в сеть запрещено. В исключительных случаях такие подключения осуществляет системный администратор с обязательным контролем этих компьютеров.

5.3. Персональные компьютеры.

- Настройка операционной системы компьютеров пользователей для корректной работы сети производится системным администратором.

Изменение конфигурации системы компьютеров, установка новых программных продуктов и аппаратных средств, изменяющих настройки системы, самостоятельно или сторонними лицами без участия системного администратора запрещено.

- Права и обязанности пользователей локальной сети регламентируются настоящим положением и должностными инструкциями.
- Отключение пользователя сети от сетевых ресурсов производится с обязательным уведомлением данного пользователя.
- При любых изменениях конфигурации подключения пользователя системным администратором производится обязательная проверка функционирования канала и доступа к ресурсам сети.
- Пользователям сети категорически запрещено передавать сторонним лицам какие-либо сведения о настройке элементов сети (имена пользователей, пароли и т. д.).
- Несанкционированное расширение пользователями своих или чужих прав запрещено.
- Запрещено изменять месторасположение компьютеров без Согласования с директором школы.

5.4. В случае нарушения установленного порядка функционирования локальной сети виновные на основании докладной записки системного администратора будут привлекаться к административной ответственности.

6. Развитие сети

6.1. Подключение к сети производится через любой телекоммуникационный канал, выбор которого осуществляется исходя из технической целесообразности.

6.2. Модернизация установленных в подразделениях компьютеров производится в плановом порядке при наличии своевременно поданной заявки и финансовых ресурсов.

О принятии мер, направленных на обеспечение защиты детей от информации, причиняющей вред их здоровью и развитию

Говорить об актуальности защиты детей от негативного воздействия Интернета, к сожалению, не приходится. В каждой школе и практически в каждой семье есть Интернет, и в подавляющем большинстве дети имеют к нему открытый доступ: более 90% несовершеннолетних являются пользователями сети Интернет, общаются в социальных сетях, ведут онлайн дневники; 73% скачивают фото, видео, музыку; 77% играют в онлайн-игры.

С 1 сентября 2011 года вступил в действие Федеральный закон от 29 декабря 2010 года N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию". Федеральный закон направлен на защиту детей от разрушительного, травмирующего их психику информационного воздействия, а также от информации, способной развить в ребенке порочные наклонности. Законом вводится запрет на информацию, вызывающую у детей страх и ужас, а также оправдывающую насилие и противоправное поведение, способную вызвать у детей желание употреблять наркотики, алкоголь или побуждающую к причинению вреда своей жизни и здоровью. Закон не преследует целей оградить детей от проблем и создать иллюзию, что в мире не существует зла, насилия, смерти. Он ставит задачу доносить до детей такого рода информацию в соответствующей их возрасту деликатной форме. Согласно данному закону полномочиями органов исполнительной власти является разработка и реализация региональных программ обеспечения информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции.

С 1 сентября 2012 года вступил в силу Федеральный закон от 28 июля 2012 года N 139-ФЗ "О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет". Этот Федеральный закон внес изменения, предполагающие фильтрацию интернет-сайтов по системе черного списка и блокировку запрещенных интернет-ресурсов.

Бесспорно, Интернет - это наш сегодняшний день и при правильном использовании дает возможность получать новые полезные знания, расширяет кругозор, но при неправильном использовании Интернет - это насилие, эротика и порнография, нецензурная лексика, информация, разжигающая расовую ненависть, пропаганда анорексии, булимии, суицида, азартных игр, наркотических веществ, экстремизма, интернет-мошенничество, педофилия, вредоносные вирусные программы.

Проконтролировать весь этот "информационный океан" невозможно.

С позиций системы образования информационная безопасность обучающихся - это необходимость:

1. обеспечивать достаточные и защищенные информационные ресурсы и информационные потоки для поддержания образовательного процесса на соответствующем уровне;
2. противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику обучающихся;
3. вырабатывать личностные и групповые навыки и умения безопасного поведения;
4. поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно не было навязано.

Таким образом, информационная безопасность детей включает две относительно самостоятельные составляющие - гуманитарную и техническую.

Техническая составляющая включает организационно-правовые механизмы и технические средства защиты.

Гуманитарная составляющая включает содержание и организацию образовательного процесса, подготовку педагогов, работу с родителями.

Проблема защиты детей от информации, причиняющей вред их здоровью и развитию, в Российской Федерации регулируется следующими нормативно правовыми актами:

- Конституция РФ от 12.12.1993;
- Федеральный закон от 24.07.1998 № 124-ФЗ "Об основных гарантиях прав ребенка в Российской Федерации";
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию";
- Федеральный закон от 13.03.2006 № 38-ФЗ "О рекламе";
- Федеральный закон от 25.07.2002 № 114-ФЗ "О противодействии экстремистской деятельности";
- Указ Президента РФ от 01.06.2012 г. № 761 "О Национальной стратегии действий в интересах детей на 2012-2017 годы";
- Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Минобрнауки РФ от 11.05.2011 № АФ-12/07 вн.

На уровне Образовательной организации

1. Вопросы использования возможностей сети "Интернет" в образовательном процессе рассмотреть на педсовете;
2. Издать приказы по вопросам обеспечения информационной безопасности

обучающихся;

3. Разработать локальные акты (Регламент доступа в сеть "Интернет", Правила использования сети "Интернет", Положение о Совете образовательной организации по вопросам регламентации доступа к информации в сети "Интернет" и др.);
4. Разработать или внести необходимые дополнения в должностные инструкции (сотрудника, назначенного ответственным за организацию работы с сетью "Интернет" и контроль доступа в сеть; учителя, допущенного к работе в сети);
5. Разработать и внедрить программы обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность.

Внешняя защищенность образовательной среды реализуется через:

- Создание системы контентной фильтрации, которая представляет собой программный комплекс, позволяющий ограничить учащимся доступ к интернет-ресурсам;
- Использование различных систем противовирусной защиты;
- Использование специальных настроек операционной системы;

Компанией ОАО "Ростелеком" в рамках договора об оказании услуг по передаче данных организована централизованная контентная фильтрация ресурсов сети "Интернет".

В качестве дополнительных средств контентной фильтрации департамент рекомендует программные продукты: Интернет цензор (<http://icensor.ru>), НетПолис (<http://www.netpolice.ru>) (для операционной системы Windows), Дансгвардиан (<http://dansguardian.org>) (для операционной системы Linux).

Еще одной мерой, направленной на обеспечение информационной безопасности детства, является создание порталов и сайтов, аккумулирующих сведения о лучших ресурсах для детей и родителей; стимулирование родителей к использованию услуги "Родительский контроль", позволяющей устанавливать ограничения доступа к сети "Интернет".

Родительский контроль - это услуга фильтрации контента, размещенного в сети "Интернет" для обеспечения доступа детей только к безопасной, проверенной информации. Информацию об услуге и способах её подключения можно получить на официальном сайте провайдера.

